IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A system for detecting intrusions, comprising:

   a) a signature computing function configured to compute a computed file signature for a file;

   b) a storage for storing a first file signature previously computed by the signature computing function for the file;

   c) a storage for storing a second file signature previously computed by other than the signature computing function for the file; and

   d) an analysis engine configured to compare the computed file signature to the first file signature and the second ~~previously computed~~ file signatures; determine the file is legitimate if the computed signature matches both the first file signature and the second file signature; and either identify the file as suspicious or subject the file to further analysis if the computed signature does not match the first file signature, the second file signature, or both.

2. (Original) The system as recited in claim 1, wherein the storage for the second previously computed file signature is a package management database.

3. (Original) The system as recited in claim 2, wherein the package management database is at a remote location from the host.

4. (Original) The system as recited in claim 2, wherein the storage for the first previously computed file signature is an internal database.

5. (Original) The system as recited in claim 4, wherein the internal database includes signatures for files previously computed by other than the signature computing function.

6. (Original) The system as recited in claim 1, wherein the first file signature is previously computed from an archival file.

7. (Currently amended) ~~A system for detecting intrusions, comprising:~~ The system as recited in claim 1, wherein the storage for the second signature is ~~a)~~ a package management database ~~including a previously computed signature for a file~~; the system further comprises ~~b)~~ a database of exceptions; and ~~c) an~~ the analysis engine is further configured to ~~compute a current signature for the file, compare the computed signature to the previously computed signature, and if there is a~~ check any mismatch between the computed signature and ~~previously computed signatures, check the mismatch~~ the second signature against the database of exceptions.

8. (Original) The system as recited in claim 7, wherein the database of exceptions includes a plurality of rules.

9. (Original) The system as recited in claim 8, wherein the database of exceptions further includes a rule categorizing some types of files as expected to change, and other types of files as expected to remain constant.

10. (Original) The system as recited in claim 9, wherein the analysis engine is further configured to use information from a file type, filename, and file type categorization to compute a suspicion level associated with a change in the file.

11. (Currently amended) A method for detecting intrusions on a host comprising the steps of:

a) providing a signature computer;

b) computing a computed signature of a file with the signature computer;

c) comparing the computed signature to a first file signature previously computed by the signature computer; ~~and~~

d) comparing the computed signature to a second file signature previously computed by other than the signature computer;

e) determining the file is legitimate if the computed signature matches both the first file signature and the second file signature; and

f) either identifying the file as suspicious or subjecting the file to further analysis if the computed signature does not match the first file signature, the second file signature, or both.

12. (Currently amended) ~~A method for detecting intrusions,~~ The method as recited in claim 11, further comprising the steps of:

a) ~~storing a previously computed signature for a file;~~

~~b)~~ providing a database of exceptions;

~~c) computing a current signature for the file;~~

~~d) comparing the computed signature to the previously computed signature;~~ and

~~e)~~ b) if there is a mismatch between the computed signature and ~~previously computed~~ the second signature~~s~~, checking the mismatch against the database of exceptions.

13. (Currently amended) A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:

a) providing a signature computer;

b) computing a computed signature of a file with the signature computer;

c) comparing the computed signature to a first file signature previously computed by the signature computer; ~~and~~

d) comparing the computed signature to a second file signature previously computed by other than the signature computer;

e) determining the file is legitimate if the computed signature matches both the first file signature and the second file signature; and

f) either identifying the file as suspicious or subjecting the file to further analysis if the computed signature does not match the first file signature, the second file signature, or both.

14. (Currently amended) A computer program product for detecting intrusions on a host as recited in claim 13, the computer program product ~~being embodied in a computer readable~~

~~medium having~~ further comprising machine readable code embodied therein for performing the steps of:

a) ~~storing a previously computed signature for a file;~~

~~b)~~ providing a database of exceptions;

~~c) computing a current signature for the file;~~

~~d) comparing the computed signature to the previously computed signature;~~ and

~~e)~~b) if there is a mismatch between the computed signature and ~~previously computed signatures~~ the second signature, checking the mismatch against the database of exceptions.